UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,975	06/25/2001	Douglas D. Boom	042390.P11657	7054

26529 7590 02/28/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN/PDC
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/886,975	BOOM, DOUGLAS D.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *30 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-13,30,31 and 46-51* is/are allowed.

6)☒ Claim(s) *14-16,18,20,22-24,26 and 28* is/are rejected.

7)☒ Claim(s) *17,19,21,25, 27 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The finality of the previous action has been withdrawn.

Response to Amendments

2. In light of the amendments made to claim 1, the Applicant has argued (page 21 last paragraph – page 22 first paragraph):

Schuba does not teach a computer comprising a network interface and a zombie detection driver coupled between, and in communication with, the network protocol and the network interface, the zombie detection driver comprising a transmit module to receive outgoing packets from a software application and discard the outgoing packets determined to be from a zombie application prior to being transmitted over a network.

...To the contrary, Schuba teaches detection and examination of TCP packets sent to a destination host by a monitor, wherein the monitor and the destination host are separate entities and the monitor monitors the TCP packets along the network.

Applicant's arguments, in light of the new amendments made to claim 1 are persuasive. Accordingly the rejection of Claims 1-9 has been withdrawn.

Furthermore, the Applicant has rewritten claims 10-13, previously objected to as being dependent on rejected claims, in independent form.

Reasons for allowance in light of these amendments are given below.

Reasons For Allowance

3. Claims 1-13, 30-31, 46-51 are held to be allowable.

Claim 1 recites:

A computer having application software in communication with a network protocol, the computer comprising a network interface and a zombie detection driver coupled between, and in communication with, the network protocol and the network interface, the zombie detection driver comprising:

- *A transmit module to receive outgoing packets from a software application and to discard the outgoing packets that are determined to be from a zombie application prior to being transmitted over a network.*

It is the Examiner's understanding that Applicant is claiming a computer having application software and a monitor such that outgoing data packets, transmitted from the purported "zombie application" are detected by the transmit module on the same computer prior to entering the network.

To this effect, the Applicant has argued that Schuba does not disclose this. Applicant asserts that Scuba monitors the TCP packets already along the network. Additionally the Applicant states that, Schuba, contrary to Applicant's invention, discloses a monitor and destination host as separate entities.

Applicant has argued: (page 21 last paragraph – page 22 first paragraph):

...To the contrary, Schuba teaches detection and examination of TCP packets sent to a destination host by a monitor, wherein the monitor and the destination host are separate entities and the monitor monitors the TCP packets along the network.

As stated above, the Applicant has claimed a transmit module which receives or "catches" outgoing data packets from an Application program or software application, and catches these packets prior to their transmission over the regular network.

Support for this interpretation is further evidenced by the Applicant's abstract within the specification

Abstract:

More particularly, the present invention monitors packets being transmitted by a computer over a network and is able to identify when these packets are part of a distributed denial of service (DDOS) attack and is able to stop the transmission of these packets before they enter the network.

In light of the Applicant's amendments, it is the Examiner's position that Schuba fails to disclose such a transmission module to further comprise the zombie detection driver, which is stated as "coupled between" the network protocol and the network interface.

No additional art has been found which discloses this limitation, nor has any motivation been found to render the invention to the limitations as claimed by the Applicant in claim 1. Accordingly, claim 1 is held to be allowable.

Claims 2-9, 30, 31 are dependent claims which depend on claim 1 or a dependent of claim 1 thereof. Accordingly, these claims are held to be allowable.

Claims 10-13, 50, previously objected to as being dependent on a rejected claim but would have otherwise been allowable have been rewritten to incorporate the subject matter of the claims from which they previously depended upon.

Claims 10-13 recite the limitation
"the zombie rating being based on whether the software application is an application or a process and whether the software application is user initiated or initiated at system startup."

While Schuba does disclose a "zombie rating" for a particular program which manages hardware which transmits outgoing data packets, the rating of Schuba is dependent upon

the behavior of particular hosts (Column 11, lines 5-15), and not whether the software application is user initiated or initiated at system startup.

No additional art has been found which discloses this limitation, nor has any motivation been found to render the invention to the limitations as claimed by the Applicant in claims 10-13.

Accordingly, claims 10-13, 50 and their dependent claims 46- 49, 51 are allowable.

Claim Objections

5. Claims 17, 19, 21, 25, 27, 29 are objected to as being dependent on a rejected claim but would have otherwise been allowable if rewritten in independent form.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 32-39, 40-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicant proceeds in claim 40 by claiming an article comprising: a storage medium having a plurality of machine accessible instructions, wherein when the instructions are executed by a processor, the instructions provide for monitoring incoming and outgoing packets to and from a software application.

However, Applicant then also claims specific action steps reciting the actions of: placing the software application, and blocking reception of incoming packets.

These actions appear to be particular actions to a method. It is indefinite because it is uncertain how these particular steps relate with the physical article which applicant has claimed..

For purposes of examination, claim 40 has been read as reciting "...the instructions provide for monitoring incoming and outgoing packets to and from a software application, said instructions further providing for the steps of:"

Claims 43, 45 are believed to have allowable subject matter if the 112 deficiency in the independent claim is corrected.

With regards to claims 32, the Applicant has recited the limitation "receive outgoing packets from a software application via the network protocol", while in the latter part of the claim, the Applicant recites that "the transmit module stops the transmission of the

outgoing packets determined to be from the zombie application before the outgoing packets are allowed to enter the network interface for transmission over the network"

The former recitation of claim 32 implies that the outgoing packets were already transmitted over a network however in that the packets were received "via the network protocol"

Claim 32 is indefinite because it claims conflicting limitations.

Claim 32 recites that outgoing packets are received via a network protocol, while also reciting that the operation of the transmit module is to stop outgoing packets before they are transmitted over the network.

Claims 33- 39 are rejected because they are dependent upon claim 32 and by incorporation by reference to their independent claim, also contain the indefinite subject matter.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 14, 15, 16, 18, 20, 22, 23, 24, 26, 28, 40-44 rejected under 35 U.S.C. 103(a) as being unpatentable over Schuba et al., US patent 6725378.

In reference to claim 14:

Schuba et al. discloses a method of detecting and restricting denial of service attacks comprising:

- Monitoring incoming and outgoing packets to and from a software application, where the monitored packets are the monitored data streams. (Column 9, lines 15-32) (Column 5, lines 58 – Column 6, line 8)
- Placing the software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets to or the software application matches that of the characteristics of a zombie application, where the zombie list is the list (Column 6, lines 30-37) from where the hosts have a rank. (Column 11, lines 8-15)
- Determining whether the software application is a known good application, wherein if the software application is not a known good application, then applying a zombie rating to the software application and if the software application is a known good application, then removing the software application from the watch list and/or zombie list, where the software application is determined to be good or bad/evil ("zombie"), and where this rating is placed as a list in a database, and where if the software application is reclassified as a good application, the good

application is removed from its status as a bad address. (Column 11, lines 50-67) & (Column 12, lines 15-32) & (Column 8, lines 18-33)

- Blocking reception and transmission of packets to and from the software application when the software application has been placed on the watch list or the zombie list in a previous cycle and the software application further exhibits the characteristics of a zombie application. (Column 11, line 65 – Column 12, line 32) & (Column 8, lines 18-33)

Schuba et al. fails to explicitly disclose a software application. Rather, Schuba monitors and classifies packets coming from specific network addresses or client systems.

However, one of ordinary skill in the art would recognize that receiving packets from a network address necessitates the packets were generated at a client computer, where the packets sent were transmitted from hardware that was operated by a control program.

For Example, if disclosure was made in which a web server receives a request for a website, one of ordinary skill in the art would recognize that the request was generated using application software such as a web browser (Internet Explorer, Netscape, Opera, Firefox).

As an additional example, Scuba et al. discloses the hardware apparatus which is operated by a set programming. (Column 7, lines 15-50)

All application programs and software inherently control and direct the use of hardware, as per the instructions dictated by its internal source code within. The advantage of using programs to control hardware is that it allows for more convenient and complex control.

It would have been obvious to one of ordinary skill in the art at the time of invention to monitor packets deriving from a software application, where the software application was operable to control a specific set of hardware to initiate the transmissions, in order to better operate and control the hardware.

In reference to claim 15:

Schuba et al. (Column 12, lines 15-32) discloses the method recited in claim 14, wherein the characteristics of a zombie application are transmitting a large number of packets while receiving no incoming packets, where an address is characterized as a bad address if a period of time has not passed without receiving an ACK packet or RST packet.

In reference to claim 16:

Schuba et al. (Column 12, lines 15-32) discloses the method recited in claim 14, wherein the characteristics of a zombie application are receiving no incoming packets and having a zombie rating exceeding a predetermined value, where the zombie rating predetermined value is the threshold when the address rating is listed as bad, as opposed to "new" or "good", where the bad rating occurs when the zombie address has not received packets for a given period of time.

In reference to claim 18:

Schuba et al. (Column 12, lines 15-32) discloses the method recited in claim 14, wherein the characteristics of a zombie application are rarely receiving incoming packets and having a zombie rating exceeding a predetermined value.

In reference to claim 20:

Schuba et al. (Column 12, lines 15-32) discloses the method recited in claim 14, wherein the characteristics of a zombie application are receiving incoming packets at first and then not receiving or sending any packets and having a zombie rating exceeding a predetermined value.

Claim 22 is rejected for the same reasons as claim 14.

Claims 23, 41 are rejected for the same reasons as claim 15.

Claim 24 is rejected for the same reasons as claim 16.

Claims 26, 42 are rejected for the same reasons as claim 18.

Claims 28, 44 are rejected for the same reasons as claim 20.

In reference to claim 40:

Schuba et al. discloses an article comprising:

- A storage medium having a plurality of machine accessible instructions, wherein when the instructions are executed by a processor, the instructions provide for monitoring incoming and outgoing packets to and from a software application; (Column 7, lines 10-33)
- Placing the software application on a zombie list or a watch list when a pattern of the incoming or outgoing packets matches characteristics of a zombie application, where the zombie list is the database, and where software applications classified as zombies are classified as "bad" in Schuba. (Column 11, lines 55- Column 12, lines 32)
- Blocking reception of the incoming packets to the software application and blocking transmission of the outgoing packets to the network when the software application has been placed on the zombie list or the watch list and the software application continues to exhibit the characteristics of the zombie application. (Column 8, lines 18-33)

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

February 3rd, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER